



Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 20 July 2004

Current Nationwide
Threat Level is



[For info click here](http://www.whitehouse.gov/homeland)
www.whitehouse.gov/homeland

Daily Overview

- Agence France Presse reports fears about terrorism returned to haunt Britain after police said they were investigating how secret security plans to prevent Heathrow airport from attack were found abandoned by a roadside. (See item [9](#))
- The New York Times reports the CIA has begun a series of terrorism briefings for state and local law enforcement personnel, for the first time dispatching counterterrorism experts to cities and small towns to warn of the possibility of an attack by al Qaeda this year. (See item [28](#))
- IDG News Service reports a virus designed to demonstrate security holes in Microsoft's Windows CE operating system, used on Pocket PCs, was identified by security companies over the weekend. (See item [29](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *July 19, Reuters* — **Oil supply fears remain.** Oil prices eased slightly but held near \$41 on Monday, July 19, as the threat of further disruption to already stretched global supplies supported prices. "Oil prices are still strong because demand is strong, capacity utilization is high, and we've still got concerns over security of supply," said Commerzbank analyst Steve Turner. **With world spare capacity at its lowest level for more than a decade, worries over**

supply disruption have kept prices well over \$35 a barrel for most of the year. In its first forecasts for next year, the Organization of the Petroleum Exporting Countries (OPEC) said on Monday it saw slower but still firm growth in worldwide appetite for oil. The oil cartel said demand for its crude would rise 340,000 barrels per day (bpd) to an average 27.36 million bpd in 2005, against an increase of 590,000 bpd this year. World oil demand would grow two percent to 82.56 million bpd in 2005, after this year's unusually sharp growth of 2.7 percent, OPEC said. OPEC, which controls 50 percent of global crude exports, is thought to be pumping at its highest levels since December 1979.

Source: http://www.washingtonpost.com/wp-dyn/articles/A61510-2004Jul_19.html

2. *July 19, Financial Post (Canada)* — **Natural gas crisis looms, study warns.** North America is heading toward an inevitable natural gas crisis that will not end until dozens of liquefied gas plants are built, according to a new study. Cambridge Energy Research Associates (CERA) says that even the prospect of new finds in Western Canada will not be enough to head off the looming crunch. Daniel Collins, CERA's associate director in Calgary, said the study was done to alert people to the expected gas crisis in which prices will hover between US\$6 and US\$7 per thousand British thermal unit at least until 2008 or 2009. The energy research institute based in Cambridge, MA, found that despite near record levels of new onshore drilling in the United States, gas production in the country continues to fall. Even exports from Canada, the U.S.'s largest foreign supplier, cannot make up the difference. **"North America's natural gas supply shortfall will challenge the North American natural gas market for the next several years,"** the study says. **"If no measures are taken to boost supply or dampen demand, North America is set to experience the highest sustained prices in the industry's history,"** it concludes.

Source: <http://www.canada.com/national/nationalpost/financialpost/story.html?id=15f57709-a7a2-4d1d-963a-a95b0751179c>

3. *July 18, Time Europe* — **Europe's power problems.** Greece's recent blackout was the most dramatic in Europe so far this year, but its electricity problems are hardly isolated. Spain, Italy, Britain, and France have all experienced significant problems. Why is Europe's electricity sector so inadequate? There are crises up and down the system: high prices, inadequate supply, creaking infrastructure. The European Commission began liberalizing the electricity market with a directive in 1996, though countries adopted rules at their own pace. Peter Claes, president of the International Federation of Industrial Energy Consumers in Geneva, Switzerland, points out that liberalization has so far accomplished very little; electricity prices have risen 35–50% in the last year despite it. Even if market liberalization were working perfectly, it alone could not add more capacity. Fatih Birol, chief economist of the Paris-based International Energy Agency (IEA), says **half the power plants in Europe are more than 25 years old, meaning they will have to be replaced in the next 15 years.** Another problem is **finding a cheap way to generate power but still abide by European Union pollution regulations and the Kyoto protocol to reduce greenhouse emissions.** There's an equally urgent need for investment in transmission and distribution, often the chief culprit in blackouts.

Source: <http://www.time.com/time/europe/magazine/article/0,13005,901040726-664983,00.html>

Chemical Industry and Hazardous Materials Sector

4. *July 19, Associated Press* — **Chemical leak in China sickens 376 people. A chemical plant in central China leaked hydrogen chloride fumes that left 56 people hospitalized and sickened 320 others, a news report said Sunday, July 18.** The emission occurred when a refrigeration compressor exploded early Saturday at the plant in the city of Kaifeng, the official Xinhua News Agency reported. The fumes wafted over a housing complex owned by company, a subsidiary of state-run China Petroleum Group, Xinhua said. It said 56 people were still being treated Sunday but gave no details of their condition or identities.
Source: <http://www.phillyburbs.com/pb-dyn/news/90-07182004-332964.ht ml>

5. *July 19, WLWT (OH)* — **Dangerous poison found in trash bin at flea market.** Visitors to a Tri-State flea market in Monroe, OH, were surprised to see men in bright orange hazardous materials clothing digging through a dumpster Sunday afternoon, July 18. **They found cyanide poison that was in both liquid and powder form, and the containers remained sealed, WLWT reported. Firefighters from Monroe and Hazmat crews from Middletown estimated that the cyanide was about 50 years old.** Authorities speculated that someone found the chemicals while cleaning out a home and disposed of them in the dumpster. The chemical, which is used to etch and color metals, is highly poisonous. About 15,000 to 20,000 people shop at the flea market each weekend, WLWT reported.
Source: <http://www.channelcincinnati.com/news/3545921/detail.html>

[[Return to top](#)]

Defense Industrial Base Sector

Nothing to report.

[[Return to top](#)]

Banking and Finance Sector

6. *July 19, Washington Post* — **Checking account fraud is increasing. Scams involving checking account fraud are on the rise, partly riding the huge increase in the volume of automated checking account withdrawals and deposits as part of the nation's wide acceptance of online banking.** The system that processes all these requests is now clearing ten billion electronic transactions a year as consumers abandon paper checks to have their payroll or Social Security funds deposited directly to their accounts or have many of their bills automatically debited from their accounts. Regulators at the Federal Reserve issued a warning to banks last year citing "alarming changes" in the automated check-clearing process. Some scammers are also using sophisticated and cheap technology to print checks and take advantage of a banking practice that allows companies to write unsigned, paper checks on a consumer's behalf for one-time transactions, such as when a consumer wants to pay a bill at the last minute or buy from a telemarketer. **Through these unsigned checks and automated withdrawals, thieves can seed thousands of bogus payment requests into that huge system, which was built on the underlying belief that the money in an individual's account is not available**

without the customer's permission.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A60345-2004Jul 18.html>

7. *July 19, eWeek* — **New phishing technique works on multiple browsers. A British Web developer has revealed a new form of a cross-site scripting, or XSS, attack that facilitates phishing activities and works on both Internet Explorer on Windows XP with Service Pack 2 (Release Candidate 2) and on the Mozilla Firefox 0.9.1 browser.** The attack allows an attacker to execute scripts in the context of another Website. After executing the attack, the user is brought to a Webpage running on the victim site (a banking site, for example), but incorporating script from the attacker site. **The main, obvious effect of the attack is that the page appears to be running in the victim site, but is incorporating elements from the attacker site. An attacker could therefore use the technique to persuade a user to provide personal information.** The effect is more difficult to detect by casual observation than many other previous phishing techniques. According to an analysis of the technique by British security consulting firm Netcraft, "having the ability to run their code from the financial institution's own site is a big step forward for fraudsters, as it makes their attack much more plausible, and will almost certainly lead fraudsters to seek out banking sites vulnerable to cross site scripting as a refinement on current phishing attacks."

Source: <http://www.eweek.com/article2/0,1759,1624751,00.asp>

8. *July 09, California Department of Insurance* — **California government computer is hacked. A California Department of Insurance (CDI) computer server, used for pre-licensing purposes, was accessed without authorization on June 30, 2004.** The Department is sending individual letters to the 599 applicants who were in the process of applying for insurance producer licenses and whose information was on the computer server at the time of the security incident. **Although the accessed computer server contained applicants' names, addresses, and social security numbers, this information was encrypted and CDI thinks it is highly unlikely that information was compromised.** CDI has taken additional security measures to prevent unauthorized accesses in the future. While CDI does not believe that private information has been revealed, it still suggests that the individuals contacted by letter order a credit report to verify that there is no unauthorized activity.

Source: <http://www.insurance.ca.gov/docs/FS-News.htm>

[\[Return to top\]](#)

Transportation Sector

9. *July 19, Agence France Presse* — **Britain on renewed terror alert after Heathrow defense plans found.** Fears about terrorism returned to haunt Britain after police said they were investigating how secret security plans to prevent Heathrow airport from attack were found abandoned by a roadside. **Documents detailing how terrorists might target the busy airport in west London, drawn up by the Metropolitan Police's air security section, were discovered by a motorist and handed into the Sun newspaper. Home Secretary David Blunkett told BBC radio that the plans appeared to be genuine.** "We have launched an internal inquiry into the circumstances of how these documents went missing and will take the appropriate action when we have ascertained the facts surrounding the matter," the Metropolitan Police said in a statement. Adding to the concern, another newspaper published an

interview with a junior government minister on Monday advising the public to stock up on food and other emergency supplies in case of a possible terror attack. While people should not "live in fear," they should make realistic preparations, anti-terrorism minister Hazel Blears told the Daily Telegraph. **Her advice came a day after the biggest anti-terrorism exercise Britain has ever seen was branded a failure when it took three hours to begin decontaminating people supposedly affected by toxic gas.**

Source: http://story.news.yahoo.com/news?tmpl=story&cid=1512&ncid=732&e=6&u=/afp/20040719/wl_afp/britain_attacks_air

10. *July 19, CNN* — **Boeing, Airbus battle for orders.** Billions of dollars in potential commercial and defense deals may be struck at the Farnborough, England bi-annual air show, which runs Monday, July 19 to Sunday, July 25, in Farnborough, southern England. As in previous shows, aerospace giants Boeing and Airbus will be battling for the spotlight and attempting to bag big orders from international carriers at a time when the industry is experiencing its worst slump in decades. **For U.S.-based Boeing, its main attention getter will be the new mid-sized 7E7 aircraft, dubbed the Dreamliner, which is due to enter service in 2008. Airbus, owned by the French group EADS, is touting its new super-jumbo A-380. The huge 555-seat aircraft is to start flying in 2006.** Japan's All Nippon Airways wants 50 of Boeing's 7E7 and another 24 airlines are considering ordering the aircraft, Reuters reported, although just four have made their intentions public. Airbus is believed to be close to A-380 deals with Turkish Airlines, Abu Dhabi-based Etihad Airways and Thai Airways, the news agency said.

Source: <http://www.cnn.com/2004/BUSINESS/07/19/farnborough.airshow/index.html>

11. *July 17, Associated Press* — **Computer glitch disrupts French trains.** A computer glitch disrupted train ticket sales across France for nearly 24 hours, delaying summer getaway plans of thousands of travelers, said the state railway operator. The computer system hang-up, whose origin was not immediately known, only affected the reservation and sale of tickets from train station ticket windows, rail operator SNCF said. **The problem, which sharply reduced use of ticket windows, started at around 9 a.m. (0700 GMT) Thursday, July 15, and was fixed by early Friday, July 16.** Sales through the Internet or on automated ticket vending machines in train stations weren't affected. Trains operated normally, but many passengers who didn't already have their tickets faced long or slow-moving lines at ticket counters. SNCF said the problem appeared to affect an exchange system linking central computers and terminals at ticket windows any time that more than 2,800 terminals were connected. Normally, about 4,400 of the terminals can be connected at any given time. The railway operator said it expected 250,000 to 300,000 passengers in France's stations between Friday and Sunday, July 18.

Source: <http://www.cnn.com/2004/TRAVEL/07/17/bt.france.train.glitch.ap/index.html>

12. *July 15, Business Travel News* — **Parker steps down as Southwest CEO, Kelly tapped as successor. In a surprise move, Southwest Airlines, on July 15, announced the resignation of CEO and vice chairman Jim Parker. Gary Kelly, previously executive vice president and CFO, was named as Parker's replacement.** Parker led the prototypical low-fare carrier since mid-2001, keeping alive Southwest's unprecedented streak of profitability — the carrier today reported its 53rd consecutive quarterly profit — and guiding its growth as it became the largest commercial carrier in the domestic system. Kelly becomes CEO, vice chairman and a member of the board of directors.

Source: http://www.btmag.com/businesstravelnews/headlines/article_d

13. *July 06, Government Accountability Office* — **GAO-04-646: Aviation Safety: Better Controls Are Needed to Improve FAA's Safety Enforcement and Compliance Efforts (Report)**. The safety of the nation's flying public depends, in large part, on the aviation industry's compliance with safety regulations and the Federal Aviation Administration's (FAA) enforcement of those regulations when violations occur. FAA attempts to gain the industry's compliance through enforcement tools, including levying fines and suspending or revoking operating certificates, and partnership programs that allow participating companies or individuals to self-report violations of safety regulations and mitigate or avoid fines or other legal actions. The Government Accountability Office (GAO) was asked to assess how FAA uses its enforcement options to address noncompliance and what management controls are in place to ensure that enforcement efforts and partnership programs result in compliance with aviation safety regulations. **GAO recommends that FAA develop evaluative processes for its enforcement efforts and partnership programs and use them to create performance goals, track performance towards those goals, and determine appropriate program changes. GAO also recommends that FAA improve the completeness of information in the nationwide enforcement database.** FAA agreed with these recommendations and provided comments on general areas covered in the report. Highlights:
<http://www.gao.gov/highlights/d04646high.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-646>

[[Return to top](#)]

Postal and Shipping Sector

14. *July 19, Bloomberg* — **Japan Post to go private in 2007. Japan Post, which holds a quarter of the nation's savings, will have to compete with banks, insurers, and other deposit-takers starting 2007, said Heizo Takenaka, Minister for Economy and Fiscal Policy.** The state-run service, which combines mail delivery with selling insurance and government-guaranteed savings, may have to break up, said Japan's guild of corporate executives. Japan's postal service held 208 trillion yen of savings at the end of March, 1.14 trillion dollars of insurance policies, one trillion dollars of government bonds and operates more branches than the nation's banks. The government may end its policy of exempting the postal service from paying taxes and may shift its collection of insurance premium, the Nikkei English News said in March. Japan's Prime Minister Junichiro Koizumi has been planning to reorganize and sell Japan Post since he first came into office in 2001. **Takenaka did not provide any details on how the sale of Japan Post will take place.** The task of selling Japan Post and changing its business may take up to 10 years to complete, Takenaka said.
Source: http://quote.bloomberg.com/apps/news?pid=100000006&sid=a_OCdYgyUBhc&refer=home
15. *July 18, Associated Press* — **Dutch postal workers ill from mail. Five Dutch postal workers became ill after handling a piece of mail containing yellow powder Sunday, July 18, police said. Police spokesperson Claudia Metz in the city of Alkmaar said the workers weren't seriously sickened, and that the powder was not anthrax.** However, she said those who came in contact with it had difficulty breathing and one mailman was briefly hospitalized

before being released. Alkmaar is around 25 miles north of Amsterdam. The mailman who was hospitalized picked the letter or package up from a public mailbox in the center of the city during his rounds. He brought it to a local distribution center where he and the others became ill.

Source: http://www3.cjad.com/content/cp_article.asp?id=/global_feeds/canadianpress/worldnews/w071849A.htm

16. *July 17, Indianapolis Star (IN)* — **Mailbox hit by explosive.** Vandals continued to plague Hendricks, IN, with the discovery Friday, July 16, of a mangled mailbox near Pittsboro. **Investigators are trying to piece together the latest explosion and to determine if this one — the sixth this month — is related to the others. The first mailbox was destroyed July 3.** Hendricks County Sheriff's Capt. Brett Clark said each mailbox was exploded using different methods, leading federal and local investigators to believe the vandals could be experimenting with different devices. They've included a pipe bomb, a PVC pipe bomb, and a carbon dioxide cartridge. On Friday, the vandals used a beer bottle and some sort of explosive. Indianapolis postal inspector Greg Beriault said it was not known what all was used in Friday's mailbox explosion, and it's too early to tell if it was related to any of the prior incidents. Results are not back yet from the Dulles, VA, laboratory where evidence from previous bombings were sent for analysis.

Source: <http://www.indystar.com/articles/3/163175-1153-009.html>

17. *July 16, Associated Press* — **FedEx to open new Kinko's. The FedEx Corp. said Friday, July 16, it will open 70 new locations for its Kinko's division in fiscal year 2005.** The package shipping giant also said in its annual report to the Securities and Exchange Commission that it expects to spend \$20 million on rebranding the new division as FedEx Kinko's Office and Print Centers. FedEx bought the Kinko's copy shop chain of 1,200 stores in February for \$2.4 billion, making it the fourth major division of the parent company. The other divisions are FedEx Express, FedEx Ground and FedEx Freight.

Source: <http://www.miami.com/mld/miamiherald/business/national/91728.03.htm?1c>

[\[Return to top\]](#)

Agriculture Sector

18. *July 19, Los Angeles Times* — **West Nile virus spreading among horses. The West Nile virus has begun to infect and kill significant numbers of horses in Southern California, especially in communities in Riverside and San Bernardino counties along the Santa Ana River, state officials said.** "We have 26 cases this year to date, all in Riverside and San Bernardino counties," said Steve Lyle, spokesman for the California Department of Food and Agriculture. "Eleven of those horses have perished." The disease appears to be spreading rapidly, with 16 of the 26 cases confirmed last week, Lyle said. There was only one case of equine West Nile virus all of last year in California. Horses cannot infect humans or other horses. When horses become infected, very few exhibit signs of clinical illness. Of those that do, about 30 percent die or must be destroyed, and another 17 percent suffer long-term debilitation. Mosquitoes transmit the disease, officials said. Horses are the domestic animal most susceptible to contracting West Nile virus, and California has one million horses — the second-largest equine population in the U.S., officials said.

Source: <http://www.latimes.com/news/local/la-me-deadhorses19jul19.1.2550332.story>

19. *July 19, Daily Nonpareil (IA)* — **Asian insect poses risk to soybeans . An insect that arrived in the U.S. in recent years and has been known to reduce soybean yields by up to 60 percent is back in Iowa fields. Clarke McGrath, an Iowa State University agronomist, said soybean aphids have started to show up in low numbers across Iowa.** Soybean aphids are native to eastern Asia and are a big problem in China, he said. They were first documented in the U.S. in 2000 and have been a big problem ever since. The aphids suck out the sap which contains the water the soybean needs to survive, McGrath said. The sap also contains all the carbohydrates the beans have picked up from the soil, and leaves the beans to respond in a manner similar to drought stress, reducing the yield. A high-speed reproduction cycle makes it difficult to get soybean aphids under control. "They have the potential to double their numbers every day and a half to two days," McGrath said. Those aphids can then double their numbers again in a similar period of time, and so on.

Source: http://www.zwire.com/site/news.cfm?newsid=12392964&BRD=2554&PAG=461&dept_id=507134&rft=6

20. *July 18, United Press International* — **Thailand to develop bird flu vaccine.** Thailand's Agriculture Minister Somsak Thepsuthin has approved an experiment on bird flu vaccines, the Bangkok Post reported Sunday, July 18. The approval moves Thailand closer to use of vaccination as an option to control the virus, which has now spread to 13 provinces. About 100,000 fowl have been culled or died in the last two weeks, when bird flu re-emerged. **Somsak said a working group of specialists in infectious diseases would conduct the experiment on the H5N1 virus strain of bird flu.** However, the Livestock Development Department is opposed to vaccine experiments. Director-general Yukol Limlaemthong says vaccination carries potential risks to public health and is unlikely to eradicate the infection.

Source: <http://washingtontimes.com/upi-breaking/20040718-060523-9258 r.htm>

21. *July 17, Daily Journal (CA)* — **Plant nurseries face challenges with quarantines. Two prime scourges menacing California's agriculture and timber industries -- the Glassy Winged Sharpshooter and Sudden Oak Death -- are putting the state's nurseries into a grip of quarantines.** "Sudden Oak Death (SOD) is creating a huge drain, and the biggest impact is on the nursery programs and nurseries themselves," said Mendocino County Agricultural Commissioner Dave Bengston. "They're so hard hit. They're already being heavily impacted, literally spending millions to cooperate with the Glassy-Winged Sharpshooter program and now they're hit by a federal quarantine on Sudden Oak Death. So these are not good times for the nursery industry." The problem is, the Glassy-Winged Sharpshooter transmits Pierce's Disease, which kills vineyards, according to Bengston. SOD is a fungus-like pathogen called *Phytophthora ramorum*. Along with killing off oak trees, SOD attacks a number of popular nursery plants, including camellias and rhododendrons. "We literally have nurseries going out of business in Southern California," Bengston said. "They're talking about potential losses to the nursery industry in the millions because of SOD and we've worried about what's going on there with SOD impacting the Glassy-Winged Sharpshooter program.

Source: <http://www.ukiahdailyjournal.com/Stories/0.1413.91~3089~2279 465.00.html>

[[Return to top](#)]

Food Sector

22. *July 16, Los Angeles Times* — **Companies charged with food safety violations. Prosecutors on Thursday, July 15, charged 10 people and four companies in Los Angeles, CA, with violating federal food safety laws in cases ranging from the alleged sale of rat-contaminated meat to the smuggling of Japanese-raised Kobe beef into the United States.** One case, dating to 2001, involves the Leonard Meat Co. of Vernon, where the U.S. Department of Agriculture seized 13,000 pounds of meat that inspectors said was contaminated with feces and showed signs of having been gnawed by rodents. In another case, the owner of a restaurant was charged with smuggling \$92,000 worth of Kobe beef into the United States. Japanese beef is barred from import because of concerns about mad cow disease. The Ariza Cheese Co. and a former supervisor were charged with shipping fresh cheese that was contaminated with listeria, a potentially lethal pathogen, from California to stores in New York in 2002. Three other cases involved the illegal import of food products that are banned because they might carry the highly contagious Newcastle virus. Three people were charged with falsifying shipping documents to smuggle from South Korea kimchee balls filled with meat and poultry. The import of meat and poultry from South Korea is prohibited because of suspected diseases.

Source: <http://www.latimes.com/news/local/state/la-me-taint16jul16.1.942976.story?coll=la-news-state>

[[Return to top](#)]

Water Sector

23. *July 18, Ledger (FL)* — **Future need for new sources of water urgent. Polk and surrounding inland Florida counties need to act quickly to develop new sources of water to meet the millions of additional gallons they will need in the future, consultants say.** The effort, which will be the outgrowth of an ongoing \$500,000, 18-month study, will look at making better use of treated sewage, tapping lakes and rivers, and finding more efficient ways to use water. **These approaches will be necessary because Southwest Florida Water Management District officials have told local officials not to expect to get much more water from the aquifer because of the damage already caused by past water withdrawals.** The Heartland Water Alliance, composed of representatives from Polk, Hardee, Highlands and DeSoto counties, was formed last year to find solutions to long-term water-supply deficits. The figures show the four counties will need 85 million gallons of water a day. In addition to tapping lakes and rivers and sewer discharges, some other alternatives include sinking wells in the South Florida Water Management District, where there are no serious water restrictions, and piping the water to users in other parts of the county.

Source: <http://www.theledger.com/apps/pbcs.dll/article?AID=/20040718/NEWS/407180400/1004>

[[Return to top](#)]

Public Health Sector

24. *July 19, JHU Gazette* — **Anthrax vaccine tests.** The Johns Hopkins Bloomberg School of Public Health is one of 12 sites testing a new vaccine to prevent anthrax. The phase II trial will evaluate the safety and immunogenic response of a new recombinant anthrax vaccine, known as rPA102. The vaccine candidate consists of recombinant protective antigen, a synthetic protein that induces antibodies designed to prevent illness by neutralizing anthrax toxins, and aluminum hydroxide to enhance the immune response. Different formulations of rPA102 will be given to 480 healthy volunteers. Each formulation will contain varying concentrations of rPA. "The goal of this study is to determine the optimal combination to induce the most robust immune response," said David Taylor, the lead investigator of the anthrax vaccine evaluation at the School of Public Health and a research professor with the Department of International Health. "If this vaccine candidate is successful, it could provide a safer vaccine for preventing anthrax with a more practical dosing schedule compared to the existing vaccine," he added. The current anthrax vaccine requires six doses administered over an 18-month period.

Source: <http://www.jhu.edu/~gazette/2004/19jul04/19anthra.html>

25. *July 16, Medical News Today* — **Oral vaccine may protect against respiratory disease. A new experimental vaccine may protect against brucellosis in humans say researchers.** Their findings appear in the July 2004 issue of the journal *Infection and Immunity*. *Brucella abortus*, *B. melitensis*, and *B. suis*, the causative agents of brucellosis in humans, are commonly acquired from infected animal products via inhalation, ingestion or traumatized skin. Although fairly well contained in the U.S., systemic infection can cause serious respiratory problems and poses great risk of morbidity worldwide. **Additionally, *Brucella* species are acknowledged by the U.S. Centers for Disease Control and Prevention as bioterror threat agents.** In the study mice were administered a live oral vaccine containing *B. melitensis* WR201 bacteria and challenged intranasally with *B. melitensis* 16M bacteria. Results showed that immunized mice were protected from infection and their lungs remained clear of bacteria.

Source: <http://www.medicalnewstoday.com/medicalnews.php?newsid=10796>

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

26. *July 19, Herald Star (OH)* — **Firefighters learn about Hazmat shelter.** Area firefighters gathered Wednesday, July 14, at the Wellsburg Fire Hall in West Virginia, to learn use of a new piece of equipment that will utilized in responding to incidents involving hazardous materials. Members of the Wellsburg, Franklin Community, WV, and Beech Bottom, WV, fire departments learned about the assembly and function of a decontamination shelter under the direction of Eldon Hagedorn, an instructor with the West Virginia University Fire Service. **Concerns about bioterrorism have led to such equipment being distributed to local fire departments throughout the U.S.** Within the collapsible tent-like structure are several shower

heads and other materials that may be used by firefighters and others wearing protective suits to remove or neutralize hazardous materials. The cost of the trailer and equipment, including decontamination suits and a computer that will be powered by a generator, has been covered by a grant from the federal Centers for Disease Control (CDC) awarded to the Brooke County Health Department and many local contributions.

Source: http://hsconnect.com/news/story/0719202004_new05news071504.a.sp

27. *July 19, Government Technology* — **New contract expands Virginia's state-wide communications system.** The Commonwealth of Virginia and Motorola Inc. have entered into a \$329 million contract to design, construct and implement state's most comprehensive statewide multi-agency radio system. **The Statewide Agencies Radio System (STARS) is built on the foundation of the recognized needs for a shared, statewide, public safety-grade radio system that includes law enforcement mobile data, and facilitates interoperability between state and local police communications systems at the city or county level.** STARS will replace the existing analog communications system used by the Virginia State Police (VSP) and other state agencies with a system that integrates radio and wireless data communications. STARS will include 130 transportable communication sites designed to be moved and placed into service anywhere within the state so as to provide state and local agencies with the additional capacity, interoperability and support for disaster-recovery operations or special events. The VSP has been tasked with facilitating the creation and implementation of the STARS project. STARS will also provide each city and county government at least one interoperability connection to the system at no cost to the localities.

Source: <http://www.govtech.net/news/news.php?id=90890>

28. *July 18, The New York Times* — **CIA sends terror experts to tell small towns of risk.** The Central Intelligence Agency (CIA) has begun a series of terrorism briefings for state and local law enforcement personnel, for the first time dispatching counterterrorism experts to cities and small towns to warn of the possibility of an attack by al Qaeda this year, government officials said. **The CIA briefings, which are being coordinated by the FBI, are conducted by intelligence analysts from the agency's Directorate of Intelligence. They have visited small cities and towns across the country, the officials said, with more meetings planned.** The center started the briefings in recent weeks to advise local authorities about the terror threat as part of an effort "to put some context and flavor into the current threat environment," which government officials have described as the most serious since the months before the September 11 attacks, the intelligence official said. The country's new acting intelligence chief, John E. McLaughlin, was the latest senior administration official to warn that the threat of terrorist attack on the United States is more significant than at any other time since September 11.

Source: <http://www.nytimes.com/2004/07/18/politics/18cia.html>

[[Return to top](#)]

Information Technology and Telecommunications Sector

29. *July 19, IDG News Service* — **First Windows CE virus emerges.** A virus designed to demonstrate security holes in Microsoft's Windows CE operating system, used on Pocket PCs, was identified by security companies over the weekend. The virus, called Duts, does not cause

any damage to systems that contract it. The WinCE4.Duts.A virus (sometimes known as Dust) only affects devices running ARM processors and infects Pocket PC PE files in the root directory, according to Bucharest-based Softwin, which first reported the virus on Saturday, July 17. It raises a dialog box which asks "Dear User, am I allowed to spread?" If the user agrees, the virus appends itself to all .EXE files not already infected in the current directory, according to anti-virus vendor Symantec Corp. **The virus was sent by its authors to anti-virus vendors rather than being distributed in the wild and was not designed to propagate on a massive scale, but rather to demonstrate that devices running Microsoft Windows CE can be infected by malicious code**, according to Viorel Canja, head of Softwin's BitDefender Labs unit. There are over 17m Pocket PCs, smartphones and other Internet appliances currently using the Windows CE operating system, according to Softwin.
Source: <http://www.pcadvisor.co.uk/index.cfm?go=news.view&news=4037>

30. *July 19, US-CERT* — **Vulnerability Note VU#303448: mod_ssl contains a format string vulnerability in the ssl_log() function.** mod_ssl is an Apache module that provides Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocol support. There is a format string vulnerability in way the ssl_log() function of the mod_ssl module handles hostnames. **By supplying a specially crafted hostname value in an HTTPS request, a remote, unauthenticated attacker could trigger this vulnerability.** Please note, the hostname provided would have to exist in the zone. A remote, unauthenticated attacker could potentially execute arbitrary code on an affected system. Upgrade to version 2.8.19–1.3.31. Alternatively, apply the appropriate vendor-specified patch: <http://www.modssl.org/source/>
Source: <http://www.kb.cert.org/vuls/id/303448>

31. *July 19, IDG News Service* — **'Deceptive Duo' hacker charged by U.S. government.** A 20-year-old man from Pleasant Hill, CA, suspected of being a hacker calling himself "the Deceptive Duo," will face a U.S. Magistrate Judge on Monday, June 19, on charges that he hacked into government computers and defaced government Websites. Robert Lyttle was indicted by a federal grand jury on Thursday, the U.S. Attorney's Office in Northern California announced Friday. **Lyttle has been charged with breaking into various government Websites in April 2002, including sites for the Department of Defense's Defense Logistic Information Service, the Office of Health Affairs, and the National Aeronautic and Space Administration's Ames Research Center.** The U.S. Attorney's Office estimated that it cost the government over \$70,000 to correct the damage caused by Lyttle. In April 2002, the Deceptive Duo claimed to be a hacking group on a mission to expose the lack of security within the U.S. government's networks as well as other private-sector computer systems. At the time of the hacking events, the Deceptive Duo said it had used a default password to log in to sites using Microsoft's SQL servers. It also breached systems by using the NetBIOS Brute Force attack method, in which a hacker repeatedly guesses passwords to gain entry into a system using the NetBIOS protocol, the group said.
Source: http://www.infoworld.com/article/04/07/19/HNdeceptiveduo_1.html

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: Microsoft has released its July Security Updates. Two of these updates are of a critical nature and should be applied to vulnerable systems. For more information, see Microsoft's bulletin here:
http://www.microsoft.com/security/bulletins/200407_windows.m.spx

Current Port Attacks

Top 10 Target Ports	135 (epmap), 137 (netbios-ns), 9898 (dabber), 5554 (sasser-ftp), 445 (microsoft-ds), 3127 (mydoom), 1434 (ms-sql-m), 1433 (ms-sql-s), 443 (https), 3128 (squid-http) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	---

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

32. *July 18, Associated Press* — **Terror insurance booms before conventions.** Insurance brokers report that more property owners are adding terror insurance to their liability coverage to insure against losses from a terror attack, thanks to the federal government's financial backing of such policies. The upcoming Democratic convention in Boston, MA, and Republican convention in New York, NY, are an opportunity for brokers in those cities to make pitches to new customers and to urge existing clients to add terrorism coverage to their policies. **Brokers say additional coverage can boost the premiums clients pay by as little as two percent in small towns and rural areas where the perceived terrorism risk is low and by 20 percent and more in the heart of Manhattan.** Terrorism coverage was practically unheard of before the September 11 attacks, and brokers say it did not become commonplace or affordable until after the Terrorism Risk Insurance Act (TRIA) took effect in November 2002. Though becoming more popular, TRIA is scheduled to expire in November 2005.

Source: http://www.washingtonpost.com/wp-dyn/articles/A59782-2004Jul_18.html

[[Return to top](#)]

General Sector

33. *July 19, Associated Press* — **Thousands flee California blaze. Dry, windy weather on Monday, July 19, hampered efforts to contain a wildfire in northern Los Angeles County that has forced thousands of people to flee their homes, one of several blazes that crews were battling in California.** Nearly 1,600 homes in Santa Clarita had been evacuated since the fire began Saturday, July 17, but there were no immediate reports of injuries or structural damage. Several hundred homes remained evacuated Monday in Sand and Placerita canyons,

said county fire Inspector Ed Osorio. More than 1,500 firefighters aided by helicopters and bulldozers were battling the 5,710-acre blaze, which was 39 percent contained Monday, July 19. The fire forced authorities to temporarily close a 10-mile stretch of the Antelope Valley Freeway east of Interstate 5. It was one of several fires around California, from eastern San Diego County to Yosemite National Park, that have burned more than 40,000 acres. A 3,600-acre fire about 90 miles east of Los Angeles in Riverside County was 50 percent contained Sunday, July 18. Elsewhere, firefighters were making steady progress against a wildfire that has been burning since July 12, about 45 miles north of Los Angeles. The arson fire has charred 17,418 acres, destroying three homes and five outbuildings.

Source: http://www.dhonline.com/articles/2004/07/18/ap/headlines/d83_tugio0.txt

[[Return to top](#)]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Alerts](#) – Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Daily Open Source Infrastructure Reports](#) – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues.

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883-3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the

informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.